IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	Civil Action No. 04-CV-1199 (SLR **FILED UNDER SEAL [REDACTED VERSION] THIS DOCUMENT CONTAINS MATERIALS WHICH ARE CONFIDENTIAL OR RESTRICTED CONFIDENTIAL - SOURCE CODE AND COVERED BY A PROTECTIVE ORDER. THIS DOCUMENT SHALL NOT BE MADE AVAILABLE TO ANY PERSON OTHER THAN THE COURT AND OUTSIDE COUNSEL OF RECORD FOR THE PARTIES**

OPENING BRIEF IN SUPPORT OF JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103 OF DEFENDANTS ISS AND SYMANTEC

Richard L. Horwitz (#2246)
David E. Moore (#3983)
POTTER ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000

OF COUNSEL:
Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600
Fax: (404) 572-5134

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation and
INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation

Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
MORRIS, JAMES, HITCHENS & WILLIAMS, LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800

OF COUNSEL:
Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Blvd.,
Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000

Attorneys for Defendant
SYMANTEC CORPORATION

Original Dated: June 16, 2006
Redacted Version: June 23, 2006

Table of Contents

TABLE OF AUTHORITIES

PAGE NO.

Cases

Statutes

I. STATEMENT OF THE CASE

In this action, SRI International, Inc. ("SRI") has sued Defendants Internet Security Systems, Inc., a Delaware corporation, Internet Security Systems, Inc., a Georgia corporation (collectively "ISS") and Symantec Corporation, a Delaware corporation ("Symantec") for patent infringement.[1] At issue are four patents relating to network intrusion detection.[2] All of the patents-in-suit claim the same priority date of November 9, 1998 and all share an almost identical written disclosure. Phillip Porras and Alfonso Valdes, employees of SRI, are the named inventors on all four patents.

The patents-in-suit generally relate to detecting attacks on computer networks, a field known as intrusion detection. There are two main facets to the patents-in-suit: (1) a hierarchy of monitors for detecting suspicious network activity, and (2) a statistical algorithm for use in detecting attacks. The '338 claims focus upon the statistical algorithm, the '203 and '615 claims focus upon the hierarchical monitor architecture, and the '212 claims include both facets.

These patents result from SRI's work on a system called EMERALD, which was funded by the United States government under the auspices of the Defense Advanced Research Projects Agency ("DARPA"). DARPA funded several projects on intrusion detection during the early-to-mid 1990s. In addition to EMERALD, DARPA also funded

---

[1] All referenced exhibits are attached to the Declaration of Renee DuBord Brown.

[2] The patents-in-suit are U.S. Patent Nos. 6,321,338 ("the '338 patent") [Ex. A]; 6,708,212 ("the '212 patent") [Ex. B]; 6,484,203 ("the '203 patent") [Ex. C]; and 6,711,615 ("the '615 patent") [Ex. D]. SRI has asserted different sets of claims against each Defendant. For convenience, the superset of asserted claims is addressed herein, which encompasses: '338 claims 1-2, 4-5, 11-13, 18-19, 24; '212 all claims (SRI has not asserted this patent against ISS, however, ISS seeks a declaratory judgment that the patent is not infringed and is invalid); '203 claims 1-9, 11-20, 22; '615 claims 1-10, 12-21, 23, 34-41, 43-51, 53. Both Defendants are currently contesting the belated attempt by SRI to add '615 claims 74 and 78, and those claims are not discussed herein.

a system called JiNao, which was developed at North Carolina State University and an associated company called MCNC. The named inventors of the patents-in-suit collaborated on JiNao. Both EMERALD and JiNao adopted a statistical algorithm that had been developed at SRI in the late 1980s/early 1990s. Both EMERALD and JiNao applied this algorithm to network traffic data. Both EMERALD and JiNao employed hierarchical network monitors.

During the course of their work on EMERALD and JiNao, the researchers shared the fruits of their government-funded research with the public by publishing detailed papers describing these systems. These public disclosures pre-date the priority filing date of the patents-in-suit by more than one year and describe all elements of the patent claims at issue. As a result, these printed publications invalidate the claims-in-suit.

SRI is not entitled to patent claims that would exclude others from practicing what had already been placed in the public domain. Under 35 U.S.C. § 102 (b), a patent is invalid if it claims inventions that were described in a printed publication more than one year before the filing date of the patent application. This rule applies equally to any public disclosure -- including prior disclosures by the very person who later seeks a patent. The patent laws are designed to promote technological advances, not takings from the public domain. *See Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 148-49 (1989). If an inventor shares his invention with the public and does not file for patent protection within one year, the invention is dedicated to the public. Here, the named inventors filed their patent application in November 1998, but described the claimed subject matter in at least two publications dated more than one year before that filing date. In addition, the developers of the JiNao system also published their paper describing the claimed subject matter more than one year before that filing date. The

inventors are therefore not entitled to patents on these claims.

The first publication by one of the named inventors, Mr. Porras, was published and presented at a national conference in October 1997. *See* P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20th National Information Systems Security Conference, October 7, 1997 ("*Emerald 1997*") [Ex. E]. This paper disclosed SRI's EMERALD project, which built upon earlier, well-known work at SRI. This paper presented the same hierarchical architecture and statistical analysis algorithms as disclosed and claimed in the patents-in-suit. The similarity between the patent specification and the *Emerald 1997* paper is striking. Entire figures and paragraphs from this paper were copied verbatim into SRI's later-filed patent specification. Even the inventors and SRI's own expert have admitted that *Emerald 1997* describes all or substantial portions of the elements of the claims of the '212, '203, and '615 patents. SRI has advanced a makeweight argument that this paper is not enabling in a belated attempt to distinguish *Emerald 1997* from the claims of the patents-in-suit. Because the patent and the paper are described at the same level of detail, these arguments simply do not rise to the level of a genuine issue of material fact and, therefore, can and should be resolved as a matter of law on summary judgment.

Both named inventors also authored and published a paper entitled *Live Traffic Analysis of TCP/IP Gateways* ("*Live Traffic*") prior to the filing date of the '338 patent. *See* P. Porras and A. Valdes, *Live Traffic Analysis of TCP/IP Gateways*, Nov. 10, 1997, http://www.sdl.sri.com/projects/emerald/live-traffic.html ("*Live Traffic*") [Ex. I]. While the final version of this paper was published in a Symposium in March 1998, an earlier draft with the same content was made publicly available on SRI's website in August

1997.[3] Because the disclosures in *Live Traffic* so clearly anticipate, SRI's only argument is whether or not it was actually "published" prior to the 102 (b) critical date or the alleged date of invention. As Defendants will show, there is no genuine issue of material fact regarding the publication date for the *Live Traffic* paper.

Finally, the publication describing the JiNao system was published in April 1997. *See* Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure*, Technical Report, April 1997 ("*JiNao Report*") [Ex. J]. The *JiNao Report* disclosed the hierarchical architecture claims of the '203, '615 and '212 patents. The *JiNao Report* also described the same statistical detection algorithm used by SRI's EMERALD system and claimed in the '338 patent. In fact, the SRI EMERALD team collaborated with the JiNao team regarding the implementation of the algorithm, as well as their related DARPA programs. Despite their collaboration with the JiNao researchers and their awareness of the *JiNao Report*, SRI's named inventors failed to disclose the *JiNao Report* to the United States Patent and Trademark Office ("US PTO").

Resolution of this case in its entirety on summary judgment is appropriate. The text of the printed publications upon which Defendants rely cannot be disputed. The dates of publication of these prior art references are beyond genuine dispute. The similarity, if not identity, of the description between these prior art publications and the patents-in-suit can also not be genuinely disputed, and have been largely conceded by the inventors and SRI's expert. In the case of *Emerald 1997* and *Live Traffic*, the prior art publications were authored by the inventors themselves to describe the very same intrusion detection system – EMERALD – described in the specification of the patents-

[3] *See* Symposium version at Ex. H, and HTML version at Ex. I.

in-suit.[4] In the case of the *JiNao Report*, the authors actually collaborated with the inventors and used the very same statistical algorithms at the heart of the system described in the patents-in-suit. Based on these undisputed facts, summary judgment of invalidity on all asserted claims should be entered.

Furthermore, this summary judgment motion does not in any way rest upon the outcome of the claim construction in this case. This unique situation is due to the fact that *Emerald 1997* and *Live Traffic* were written by the inventors about the same system discussed in the patents-in-suit, and thus the language used is virtually identical. Similarly, the *JiNao Report* also uses similar language to describe the JiNao statistical algorithms because the JiNao team used the same algorithms as SRI disclosed in the patents-in-suit. Thus, the references relied upon herein are invalidating references regardless of whether SRI's or the Defendant's proposed constructions are adopted.

II. SUMMARY OF THE ARGUMENT

1. The *Emerald 1997* publication anticipates pursuant to 35 U.S.C. § 102 (b) the '212, '203, and '615 asserted claims.

2. In the alternative, *Emerald 1997* in combination with *Intrusive Activity 1991* renders obvious pursuant to 35 U.S.C. § 103 the '203 and '615 asserted claims.

3. The *Live Traffic* publication anticipates pursuant to 35 U.S.C. § 102 (a) and (b) the '338, '212, '203 and '615 asserted claims.

4. In the alternative, *Live Traffic* in combination with *Emerald 1997* renders obvious pursuant to 35 U.S.C. § 103 the '212 claims 6, 13, 17 and 24; '203 claims 4, 11, 15 and 22; and '615 claims 4, 12, 16, 23, 37, 43, 47, and 53.

---

[4] To the extent there are claims with limitations that are not explicitly described in the references, those limitations would have been inherent in the disclosure or obvious additions to that disclosure. Indeed, the named inventors themselves pointed to combining EMERALD with the additional reference relied upon herein for the obviousness showing of certain limitations: L.T. Heberlein et al., *A Method to Detect Intrusive Activity in a Networked Environment*, 14th National Computer Security Conference, Oct. 1-4, 1991 ("*Intrusive Activity 1991*") [Ex. F].

5. The *JiNao Report* anticipates pursuant to 35 U.S.C. § 102 (b) the '338, '212, '203 and '615 asserted claims.

III. STATEMENT OF FACTS

A. BACKGROUND REGARDING INTRUSION DETECTION

1. The history of the intrusion detection field

Intrusion detection systems ("IDS") are designed to detect, and in some cases thwart, unwanted attempts to infiltrate or access a computer or computer network. An "intrusion" can refer to any type of anomalous, illicit, or prohibited activity. An intrusion may originate from an external threat, or misuse by an internal user. IDS has been described as "a burglar alarm for computers and networks." R. Bace, INTRUSION DETECTION at 7 (Macmillan Technical Publishing 2000) [Ex. Z]. Like any technology, the IDS field has evolved over time. In order to provide a context for understanding the claimed inventions, this section provides a short overview of the history of the IDS field.

The U.S. government has played an important role. Beginning in the 1970's, the Department of Defense ("DOD") funded a "trusted systems" initiative to provide computer system security for the processing of classified information. As part of this program, the DOD created a policy for implementing certain auditing functions for computers to track behavior and discover potential security problems. *See* R. Bace, INTRUSION DETECTION at 11 [Ex. Z]. An audit trail (also known as an "audit log") is a record showing who has accessed a computer system and what operations he or she has performed during a given period of time. An audit trail may track basic operating system functions, such as system calls and processes performed, or it may track application usage or data access.[5]

[5] For an overview regarding audit trails, *see* S. Garfinkel and G. Spafford, PRACTICAL

Many early IDS systems focused upon the analysis of audit trail information. Such analysis is sometimes referred to as "host-based" because it relies upon information generated on a particular "host" or computer. However, with the proliferation of large computer networks and the likelihood of network-based attacks increasing, IDS systems began focusing upon network traffic and network sources for attack. For example, in the early 1990's, the Network Security Monitor ("NSM") developed at the University of California at Davis targeted computer networks and analyzed packet data. *See id.* at 18-19 [Ex. Z]; L.T. Heberlein et al., *A Network Security Monitor,* Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, at 296-304, Oakland, C.A., May 7-9, 1990 [Ex. NN].

As the inventors of the patents-in-suit have acknowledged, analysis of packet data in the context of network monitoring is quite old, and has been studied extensively in both the IDS field and many other areas of computing.[6] Packet-switched networks were first developed by the DOD for the Advanced Research Projects Agency Network ("ARPANET") in the late 1960s, which eventually formed the backbone of the Internet we know today. In the 1970-80s, early Internet researchers began developing a standard communication protocol for the Internet. This protocol suite became known as TCP/IP ("Transmission Control Protocol/Internet Protocol").[7]

UNIX & INTERNET SECURITY at 289-92 (O'Reilly and Assoc. 2nd ed. 1996) [Ex. AA].

[6] The inventors have stated in their publications that the concepts of network monitoring and the use of packet monitoring in IDS were not new at the time of the alleged inventions. *See* P. Porras and A. Valdes, *Live Traffic* at 3 (noting that "[n]etwork monitoring, in the context of fault detection and diagnosis for computer network and telecommunication environments, has been studied extensively by the network management and alarm correlation community" and "[b]oth [the NSM and NADIR systems] performed broadcast LAN packet monitoring to analyze traffic patterns for known hostile or anomalous activity") [Ex. I].

[7] *See* B. M. Leiner et al., A Brief History of the Internet,

In conjunction with the growth of the Internet, a wide variety of different types of computer and networking hardware were developed to handle the routing, monitoring, and filtering of network traffic and network packets. For example, routers and gateways were developed to connect computer networks. Routers and gateways receive packets and forward them to their correct destinations based upon the address in each packet's header.[8] As the need for securing networks, especially those connected across the Internet, became apparent, "firewalls" were developed in the early 1990's to provide a mechanism to filter and block unwanted packets and traffic.[9] Firewalls and the information they generate serve as important data sources for IDS systems.[10]

2. History of SRI's IDES, NIDES and EMERALD projects

SRI, in conjunction with various government research efforts, has worked and published in the IDS field for more than 20 years. Much of this published work involves a system that has undergone three different evolutions over time: IDES, NIDES, and EMERALD. As the inventors themselves have explained:

> Our earlier intrusion-detection efforts in developing IDES (Intrusion Detection Expert System) and later NIDES (Next-Generation Intrusion Detection Expert System) were oriented toward the surveillance of user-session and host-layer activity. This previous focus on session activity within host boundaries is understandable given that the primary input to intrusion-detection tools, audit data, is produced by mechanisms that tend

---

http://www.isoc.org/internet/history/brief.shtml (last visited June 15, 2006).

[8] Although these two terms have been used synonymously, a gateway has also been defined as connecting networks using different communication protocols. *See* definitions of "router" and "gateway" in COMPUTER DICTIONARY, Microsoft Press 3rd ed. (1997) [Ex. LL].

[9] *See* Avolio Decl., ¶ 24 [Ex. X].

[10] "Many firewalls, I&A systems, access control systems, and other security devices and subsystems generate their own activity logs. These logs contain information that is, by definition, of security significance; they are therefore of particular value to the intrusion detection process. Including these logs as information sources is an obvious way to improve the quality of the intrusion detection process." R. Bace, INTRUSION DETECTION at 74 [Ex. Z].

> to be locally administered within a single host, or domain. However, as the importance of network security has grown, so too has the need to expand intrusion-detection technology to address network infrastructure and services. In our current research effort, EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances), we explore the extension of our intrusion-detection methods to the analysis of network activity.

Live Traffic at 3 [Ex. I]. Different authors at SRI, including the named inventors for the patents-in-suit, published extensively on IDES, NIDES, and EMERALD prior to filing the '338 patent.[11]

In the late 1980s, SRI began working on IDES – a system to observe computer behavior and learn to recognize "normal" behavior and deviations from normal behavior. *See* H. Javitz and A. Valdes, *The SRI IDES Statistical Anomaly Detector*, 1991 IEEE Computer Society Symposium on Research in Security and Privacy (May 1991) [Ex. GG]. The statistical anomaly detection algorithm used by SRI in all of its IDS work was developed as part of IDES. SRI's "next-generation" of the IDES project, NIDES, furthered this work. *See* R. Jagannathan et al. (including A. Valdes), *System Design Document: Next-Generation Intrusion Detection Expert System (NIDES)*, March 9, 1993 at 55 [Ex. HH]. NIDES used the IDES statistical profiling algorithms to monitor computer information for deviations from normal computer activity. NIDES also included the use of a rule (or signature) based expert system to detect known attacks. *Id.* at 2-4, 31 [Ex. HH]. NIDES had a modular architecture that included two analysis engines (statistical and signature) and a resolver to combine the results of the two engines. *Id.* at 2-4 [Ex. HH].

IDES and the original NIDES were primarily host-based systems, deriving their information from audit data. As the use of networking expanded and other intrusion

---

[11] *See* Ex. N, listing many different SRI publications on IDES, NIDES, and EMERALD,

detection systems began to look at network traffic and large networks, SRI sought government funding to create a successor to NIDES that would monitor network traffic. This system was eventually called EMERALD.

By December 1996, SRI had published a conceptual overview of the EMERALD system, *see* P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances, Conceptual Overview,* http://www.sdl.sri.com/papers/emerald-position1/ (December 18, 1996) [Ex. JJ], and by October 1997, SRI had fully disclosed the EMERALD system in the *Emerald 1997* publication. Like NIDES, EMERALD employed a modular component architecture called a "monitor" that included a statistical profiling engine and a signature-based engine with a resolver to combine the results from the two engines.

The *Emerald 1997* paper disclosed the details of the analysis hierarchy of monitors and the statistical detection method claimed in the patents-in-suit. Indeed, the similarities between *Emerald 1997* and the common patent specification are extensive. For example, Fig. 1 from *Emerald 1997* is virtually identical to the patents' Fig. 2.[12] In addition, Fig. 2 from *Emerald 1997* is identical to the patents' Fig. 3.[13] There are numerous examples in which the language of *Emerald 1997* can be found verbatim in the patents' specification.[14] Both *Emerald 1997* and the patents-in-suit also state that they were funded by the same contract from DARPA.[15]

---

all dated more than one year prior to November 9, 1998.

[12] *Compare Emerald 1997*, Fig. 1 at p. 357, with '338 Fig. 2 and col. 3:4-5.

[13] *Compare Emerald 1997*, Fig. 2 at p. 358, with '338 Fig. 3 and col. 3:6-7.

[14] *See* comparison of *Emerald 1997* to '338 common patent specification [Ex. W].

[15] DARPA contract F30602-96-C-0294.

The next paper describing EMERALD was the *Live Traffic* paper. This paper had a similar disclosure to *Emerald 1997* and added further details on specific types of network traffic analysis. In August 1997, one of the inventors, Mr. Porras, posted copies of *Live Traffic* on SRI's ftp site and on SRI's worldwide website. [16] In March 1998, *Live Traffic* was published at the Internet Society's Networks and Distributed Systems Security Symposium.[17] Like *Emerald 1997*, *Live Traffic* shares overlapping text and figures with the patents-in-suit.

3. History of JiNao

The *JiNao Report* also stems from work related to SRI's NIDES project. The EMERALD and JiNao projects were both government projects funded by DARPA reporting to the same Program Manager.[18] The JiNao team used SRI's NIDES statistical algorithms for analysis – the same algorithms the patents-in-suit refer to as being suitable for use in the patented system. *See JiNao Report* at 18 [Ex. J] and '338 col. 5:42-48 [Ex. A]. Multiple meetings between the named inventors and the JiNao team occurred at which the use of the NIDES algorithms was discussed.[19] Reports on EMERALD for the U.S. Government written by the inventors confirm that the inventors provided information on the EMERALD statistical component to the JiNao team.[20]

Like EMERALD, the disclosed JiNao system included an analysis hierarchy of monitors, where each monitor used a statistical-based and a rule-based analysis engine.

---

[16] Porras 30(b)(6) Tr. 110-22 [Ex. T]; *see also* Ex. I.

[17] *See* Ex. H.

[18] Porras 30(b)(6) Tr. 96-100 [Ex. T]; Jou Tr. 96-97 [Ex. R]; Lunt Tr. 16-17; 80-81 [Ex. KK].

[19] Jou Tr. 30-31, 39-42, 66-67, 69-70 [Ex. R]; Porras Tr. 163, 174-75 [Ex. T]; Valdes Tr. 86-88, 156-57 [Ex. U].

[20] *See* SRI 011739-43 at SRI 011742 and SRI 012308-404 at SRI 012400 [Ex. EE]; *see*

Like EMERALD, JiNao applied the NIDES statistical detection algorithm to network traffic data.

B. THE ALLEGED INVENTIONS OF THE PATENTS-IN-SUIT

The common specification of the patents-in-suit describes a hierarchical scheme for the monitoring and analysis of networks for the purpose of intrusion detection.[21] The specification describes two different types of "analysis engines" for the network monitors: a "profiler engine" which uses a particular statistical technique, and a "signature engine." The '338 claims focus upon statistical profiling, which the specification explains uses SRI's prior techniques from the NIDES program:

> The profile engine 22 may use a statistical analysis technique described in A. Valdes and D. Anderson, "Statistical Methods for Computer Usage Anomaly Detection Using NIDES", Proceedings of the Third International Workshop on Rough Sets and Soft Computing, January 1995, which is incorporated by reference in its entirety.

'338 col. 5:42-48 [Ex. A].[22] The '203 and '615 claims do not require statistical techniques, but instead focus upon a hierarchical monitoring scheme of monitors feeding information to higher-level monitors.[23] The '212 patent requires the use of a "statistical detection method" but also requires a hierarchical monitoring scheme.

---

also Jou Tr. 30-31, 47, 67 [Ex. R].

[21] The patents share a common specification, which also internally references two different articles: (1) A. Valdes and D. Anderson, *Statistical Methods for Computer Usage Anomaly Detection Using NIDES (Next-Generation Intrusion Detection Expert System)*, Proceedings of the Third International Workshop on Rough Sets and Soft Computing, p. 306-11, Jan. 27, 1995 (referenced at '338 col. 5:44-48) ("*Statistical Methods*") [Ex. FF] and (2) P. Porras and A. Valdes, *Live Traffic Analysis of TCP/IP Gateways*, 1998 ISOC Symposium on Network and Distributed Systems Security, March 1998 (referenced at '338 col. 12:61-65) [Ex. H]. The text of this Symposium proceeding is the same as the earlier HTML version of the same *Live Traffic* paper discussed herein. [Ex. I]. SRI has admitted that neither of these articles constitute "essential material" for purposes of satisfying 35 U.S.C. § 112. *See* SRI's Responses to Defendant Symantec's First Set of Requests for Admission [Nos. 1-4] [Ex. Q].

[22] This publication is referred to herein as *Statistical Methods, see* Ex. FF.

The specification describes an enterprise network which includes a set of "network monitors" for analyzing network activity. '338 col. 3:32-35 [Ex. A]. These monitors are deployed in a hierarchy and include lowest-level "service monitors," as well as "domain monitors" and "enterprise monitors." The service monitors analyze data from network traffic / network packets handled by "network entities" such as gateways, routers, or firewalls. '338 col. 3:42-45 [Ex. A]. The service monitors produce reports and disseminate them to other monitors via a subscription-based distribution scheme. '338 col. 3:55-65 [Ex. A].

Each monitor can analyze "event records that form an event stream." '338 col. 4:61-62 [Ex. A]. Event records can be created from raw network traffic / network packets. As the specification states, the selection of data from the packets for analysis can be based upon different criteria. '338 col. 4:61-5:5 [Ex. A]. The analysis engines of the monitors receive the event records. '338 col. 5:34-35 [Ex. A].

Each monitor includes one or more analysis engines, including a "signature analysis engine" and a "statistical analysis engine," which perform different types of analysis on the data collected by the monitors. *See* '338 Fig. 2 [Ex. A]. The signature engine looks for known patterns of attack in the event stream. For example, this engine can perform a threshold analysis, which detects when the number of occurrences of a specific event exceeds a preset level. '338 col. 7:24-26, 7:45-55 [Ex. A]. By contrast, the statistical engine performs statistical profile-based anomaly detection where the pattern of attack may not be known. The statistical engine uses "statistical measures to profile network activity indicated by an event stream." '338 col. 7:36-38 [Ex. A]. Statistical measures are variables created from event records. These measures are used to create

---

[23] With the exception of '615 claim 7, which requires a "statistical detection method."

both a long-term and a short-term statistical profile. '338 col. 6:38-50 [Ex. A]. While the long-term statistical profile characterizes historical activity, the short-term statistical profile "characterizes recent activity." '338 col. 6:44-47 [Ex. A]. The short-term profile is compared to the long term profile to determine if recent activity is anomalous. '338 col. 6:38-7:3 [Ex. A].

The specification mentions that hierarchical domain monitors correlate reports from service monitors and distribute their reports to enterprise monitors. '338 col. 3:66-4:18 [Ex. A]. In turn, hierarchical enterprise monitors correlate reports across their set of monitored domains. '338 col. 4:18-47 [Ex. A]. However, no description of how this "correlation" is performed is provided.

C. THE ASSERTED CLAIMS

Many of the asserted claims are duplicative. For example, although each patent has both method and apparatus claims, the limitations of each are virtually identical (*see, e.g.*, '338 claims 1 and 24).

The '338 patent claims focus on the statistical anomaly detection algorithm. Claim 1 is representative of the independent claims:

> 1. A method of network surveillance, comprising:
>
> receiving network packets handled by a network entity;
>
> building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections;
>
> comparing at least one long-term and at least one short-term statistical profile; and
>
> determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.

All three of the "hierarchical" patents ('212, '203 and '615) are extremely redundant.[24] The '203 patent claims focus on the analysis hierarchy of monitors for detecting suspicious network activity. The '203 patent requires that at least one type of particular "network traffic data categories" be used for the analysis. The '203 patent does not require any particular detection method (*i.e.*, the suspicious network activity may be detected using either statistical or signature methods). Claim 1 is representative of the alleged invention claimed:

> 1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:
>
> deploying a plurality of network monitors in the enterprise network;
>
> detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};[25]
>
> generating, by the monitors, reports of said suspicious activity; and
>
> automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.

The '615 claims are almost exactly the same as the '203 claims. '615 claim 1 merely adds two additional categories of network traffic data: "network connection acknowledgments" and "network packets indicative of well-known network-service protocols."

The '212 claims are also very similar to the '203 and '615 claims. The '212 claims do not require use of any of the particular "network traffic data categories" from '203 claim 1. Instead, the '212 claims require that at least one of the network monitors

---

[24] *See* Ex. CC, which compares claim 1 of the '212, '203, and '615 patents, and highlights the two limitations where these claims differ.

[25] In order to invalidate this limitation, a prior art reference need only disclose one of the claimed "network traffic data" categories.

utilize a "statistical detection method." In addition, '212 claims 2 and 3 further require the use of a "signature matching detection method."

D. THE SUMMARY OF ESTABLISHED FACTS

1. The priority filing date for all of the patents-in-suit is November 9, 1998.
2. *Emerald 1997* was publicly available more than one year prior to November 9, 1998.[26]
3. *Live Traffic* (HTML version) was publicly available more than one year prior to November 9, 1998.[27]
4. *Live Traffic* (Symposium version) was publicly available prior to November 9, 1998.[28]
5. *Intrusive Activity 1991* was publicly available more than one year prior to November 9, 1998.[29]
6. *JiNao Report* was publicly available more than one year prior to November 9, 1998.[30]
7. *Emerald 1997* discloses all of the limitations of the '212 asserted claims.[31]
8. *Emerald 1997* discloses monitoring network datagrams (a synonym for network packets).[32]

---

[26] SRI has admitted that *Emerald 1997* was published on October 9, 1997. *See* Plaintiff SRI's Responses to Defendant ISS's First Set of Requests for Admission, Request No. 1 [Ex. O].

[27] *See supra* Part IV.C.1.

[28] *See* Ex. H; see also '338 col. 12:61-65 [Ex. A].

[29] SRI has admitted that *Intrusive Activity 1991* was publicly available prior to November 1997, *see* SRI's Responses to Symantec's Third Set of Requests for Admission [Ex. P].

[30] The author of the *JiNao Report*, Mr. Jou, testified that he made the document available on the MCNC website in April 1997. Jou Tr. 73-87 [Ex. R]. A declaration from the Internet Archive confirms that the *JiNao Report* was publicly available prior to November 1997. *See* Internet Archive Decl. at ISS_02125906, ISS_ 02125910 (illustrating that the *JiNao Report* was posted on the MCNC website at least as early as 08/01/1997) [Ex. S]. Furthermore, Mr. Jou testified he emailed a link to this document to many researchers in the intrusion detection field in April 1997, including both named inventors. Jou Tr. 75-77; Jou Exhibit 17 (SRIE 0399295) [Ex. R].

[31] Valdes Tr. 466-67 [Ex. U]; chart comparing *Emerald 1997* to '212, '203, and '615 asserted claims [Ex. K]; *see also supra* Part IV.B.1.

[32] Emerald 1997 at 356.

9. *Emerald 1997* discloses monitoring firewalls and activity logs.[33]

10. Firewalls in 1997 were well-known network monitoring tools that monitored "network connection requests," "network connection denials," and "network packet data volume."[34]

11. Firewall logs in 1997 logged for review records of "network connection requests," "network connection denials," and "network packet data volume."[35]

12. One of ordinary skill in the art would have been motivated to combine *Emerald 1997* with its cited reference *Intrusive Activity 1991* to determine what measures of network datagrams/packets to monitor.[36]

13. *Intrusive Activity 1991* discloses analysis of "network packet data volume," "network connection requests," and "network connection denials."[37]

14. *Emerald 1997* alone and in combination *with Intrusive Activity 1991* discloses all of the limitations of the asserted '203 and '615 claims.[38]

15. *Emerald 1997* is an enabling reference for the asserted claims of the '212, '203, and '615 patents.[39]

16. *Live Traffic* discloses all of the limitations of the asserted claims.[40]

17. One of ordinary skill in the art would have been motivated to combine *Live Traffic* with its cited reference *Emerald 1997*.[41]

18. *Live Traffic* is an enabling reference for the asserted claims.[42]

19. *JiNao Report* discloses all of the limitations of the asserted claims.[43]

---

[33] *Emerald 1997* at 354, 355 [Ex. E]; Avolio Decl. ¶¶ 49-56 [Ex. X].

[34] Avolio Decl. ¶¶ 21-27, 35-41, 60-78 [Ex. X].

[35] Avolio Decl. ¶¶ 35-41, 63, 67-71, 73-75, 79 [Ex. X].

[36] Kesidis Tr. 673-76 [Ex. V]; *see also supra* Part IV.B.2.b.

[37] *Intrusive Activity 1991* at 368-69, 365, 370 [Ex. F]; *see also supra* Part IV.B.2.b.

[38] Chart comparing *Emerald 1997* to '212, '203, and '615 asserted claims [Ex. K]; *see also supra* Part IV.B.2.

[39] Heberlein Decl. ¶¶ 86-93 [Ex. Y].

[40] Chart comparing *Live Traffic* to asserted claims [Ex. L]; *see also supra* Part IV.C.

[41] *See supra* Part IV.C.2.

[42] Heberlein Decl. ¶¶ 86-93 [Ex. Y].

[43] Chart comparing *JiNao Report* to the asserted claims [Ex. M]; *see also supra* Part IV.D.

20. *JiNao Report* is an enabling reference for the asserted claims.[44]

IV. SUMMARY JUDGMENT OF INVALIDITY SHOULD BE ENTERED ON ALL OF THE ASSERTED CLAIMS

A. LEGAL STANDARDS

1. Summary judgment

Summary judgment is appropriate if "no genuine issue exists as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). "Facts that could alter the outcome are material, and disputes are genuine if evidence exists from which a rational person could conclude that the position of the person with the burden of proof on the disputed issue is correct." *Matsushita Elec. Indus. Co. v. Cinram Int'l, Inc.*, 299 F. Supp. 2d 348, 357 (D. Del. 2004) (citations omitted). The moving party bears the burden of proving that no genuine issue of material fact exists. *See Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586 n.10 (1986). If the moving party proves an absence of material fact, the nonmoving party "must come forward with 'specific facts showing that there is a genuine issue for trial.'" *Matsushita*, 475 U.S. at 587 (quoting Fed. R. Civ. P. 56(e)).

2. Anticipation under 35 U.S.C. § 102

"A patent is invalid for anticipation when the same device or method, having all the elements contained in the claim limitations, is described in a single prior art reference." *Crown Operations Int'l, Ltd. v. Solutia, Inc.*, 289 F.3d 1367, 1375 (Fed. Cir. 2002). Anticipation is a question of fact, *see In re King*, 801 F.2d 1324, 1326 (Fed. Cir. 1986), and must be proven by clear and convincing evidence. *See Norian Corp. v. Stryker Corp.*, 363 F.3d 1321, 1326 (Fed. Cir. 2004). Despite being a question of fact,

[44] Heberlein Decl. ¶¶ 94-95 [Ex. Y].

summary judgment of anticipation is appropriate if the record reveals no genuine dispute of material fact. *See General Electric Co. v. Nintendo Co., Ltd.*, 179 F.3d 1350, 1353 (Fed. Cir. 1990); *see also Telemac Cellular Corp. v. Topp Telecom, Inc.*, 247 F.3d 1316, 1327 (Fed. Cir. 2001).

In order to anticipate, a prior art disclosure must enable one of skill in the art to practice the invention without undue experimentation. *See Novo Nordisk Pharm., Inc. v. Bio-Tech. Gen. Corp.*, 424 F.3d 1347, 1355 (Fed. Cir. 2005). Whether a prior art reference is enabled is a question of law based on underlying factual findings. *Id.* at 1342-43. The patentee bears the burden to show that a prior art reference is not enabled. *See Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1355 (Fed. Cir. 2003) (regarding a prior art patent); *Novo Nordisk Pharm., Inc. v. Bio-Tech. Gen. Corp.*, 2004 U.S. Dist LEXIS 14960 at *73 (D. Del. 2004) (regarding non-patent prior art) *aff'd in part and vacated in part*, 424 F.3d 1347 (Fed. Cir. 2005).

Where the reference has previously been considered by the US PTO Examiner, an element of deference is given to the decision of the examiner. *American Hoist & Derrick Co. v. Sowa & Sons, Inc.* 725 F.2d 1350, 1358-59 (Fed. Cir. 1984). However, the law recognizes that there are references previously considered by an Examiner which contain "disclosure so poignantly impacting upon patentability as to render virtually irrelevant the fact of its consideration by the examiner." *Lear Siegler, Inc. v. Aeroquip Corp.*, 733 F.2d 881, 886 n.4 (Fed. Cir. 1984). Given the closeness of the *Emerald 1997* and *Live Traffic* disclosures to the claims of the patents in question (including complete identity of several figures), the overlap in authorship, and the Examiner's complete silence on all prior art issues during prosecution of all of the patents-in-suit, *Emerald 1997* and *Live*

Traffic are such references.[45]

A prior art reference may anticipate without expressly disclosing a particular limitation if that limitation is inherently present in the reference. *Glaverbel Societe Anonyme v. Northlake Mktg. & Supply, Inc.,* 45 F.3d 1550, 1554 (Fed. Cir. 1995). Whether or not a limitation is inherent in a reference is a question of fact. *See In re Schreiber*, 128 F.3d 1473, 1477 (Fed. Cir. 1997). Anticipation is viewed through the perspective of one of ordinary skill in the art. Thus, in making a determination of inherent anticipation, extrinsic evidence may be considered "to explain the disclosure of a reference. … The role of extrinsic evidence is to educate the decision-maker to what the reference meant to persons of ordinary skill in the field of the invention, not to fill gaps in the reference." *Scripps Clinic & Research Found. v. Genentech, Inc.*, 927 F.2d 1565, 1576 (Fed. Cir. 1991).[46] As the Federal Circuit has explained:

> To serve as an anticipation when the reference is silent about the asserted inherent characteristic, such gap in the reference may be filled with recourse to extrinsic evidence. Such evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. …This modest flexibility in the rule that 'anticipation' requires that every element of the claims appear in a single reference accommodates situations where the common knowledge of technologists is not recorded in the reference; that is, where technological facts are known to those in the field of the invention, albeit not known to judges.

Continental Can Co. v. Monsanto Co., 948 F.2d 1264, 1268-69 (Fed. Cir. 1991) (citations omitted). Thus, extrinsic evidence may be used to explain but not expand the meaning of

---

[45] The Examiner did not issue a single Office Action on any piece of prior art for any of the four patents-in-suit.

[46] *See also Ciba-Geigy Corp. v. Alza Corp.*, 864 F. Supp. 429 (D. N.J. 1994) (finding a letter to the editor of Nature an anticipatory reference, relying in part upon an expert declaration attesting to the understanding one of skill in the art), *aff'd in part, vacated in part, and remanded* in unpublished opinion, 37 U.S.P.Q.2d 1337 (Fed. Cir. 1995) [Ex. II].

a reference. *See In re Baxter Travenol Labs.*, 952 F.2d 388, 390 (Fed. Cir. 1991); *AT&T Corp. v. Excel Communications, Inc.*, 1999 U.S. Dist. LEXIS 17871 (D. Del. 1999).

3. Obviousness under 35 U.S.C. § 103

A patent claim is invalid for obviousness under 35 U.S.C. § 103 if the differences between it and the prior art are such that the claimed subject matter as a whole would have been obvious to one of ordinary skill in the art at the time the invention was made. *See Union Carbide Plastics & Tech. Corp. v. Shell Oil Co.*, 308 F.3d 1167, 1187 (Fed. Cir. 2002). The ultimate determination of whether an invention would have been obvious is a legal conclusion based on the totality of the evidence, including underlying factual inquires. *See Tegal Corp. v. Tokyo Electron America, Inc.*, 257 F.3d 1331, 1348 (Fed. Cir. 2001). There are typically four underlying factual inquiries: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) any objective indicators of non-obviousness, more commonly termed secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966); *B.F. Goodrich Co. v. Aircraft Braking Sys. Corp.*, 72 F. 3d 1577, 1582 (Fed. Cir. 1996). Where a legal conclusion of obviousness is disputed, but the underlying facts are not, there is no issue of fact requiring a trial and summary judgment is appropriate. *See Newell Cos. v. Kenney Mfg. Co.*, 864 F. 2d 757, 763 (Fed. Cir. 1988). In addition, summary judgment on the basis of obviousness may be granted to invalidate patent claims when the subject matter of the invention and the prior art are so readily understandable as to eliminate any genuine issue of fact. *See Union Carbide Corp. v. American Can Co.*, 724 F.2d 1567, 1573 (Fed. Cir. 1984).

The existence of each limitation of a claim in the prior art does not, by itself, demonstrate obviousness. Instead, there must be a "reason, suggestion, or motivation" to

combine the references. S*miths Indus. Med. Sys., Inc. v. Vital Signs, Inc.*, 183 F. 3d 1347, 1353 (Fed. Cir. 1999).

> [T]he motivation-suggestion-teaching test asks not merely what the references disclose, but whether a person of ordinary skill in the art, possessed with the understandings and knowledge reflected in the prior art, and motivated by the general problem facing the inventor, would have been led to make the combination recited in the claims.

In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006). Obviousness can be found on the basis of a "problem [that] was within the general knowledge of those of ordinary skill in the art," even if the patent is not directed at "the identical problem addressed in [the] prior art." *Cross Medical Products, Inc. v. Medtronic Sofamor Danek, Inc.*, 424 F.3d 1293, 1322-23 (Fed. Cir. 2005).

B. EMERALD 1997 ANTICIPATES AND RENDERS OBVIOUS THE ASSERTED CLAIMS

Emerald 1997 expressly anticipates or inherently anticipates all of the asserted claims of the '212, '203, and '615 "hierarchical" patents. In addition, *Emerald 1997* in combination with an internally-cited reference also renders obvious the asserted claims of the '203 and '615 patents. The chart at Exhibit K provides the relevant disclosures from *Emerald 1997* for both anticipation and obviousness for each of the claim limitations.

This is a somewhat unusual case in that Alfonso Valdes, a named inventor, admitted that *Emerald 1997* disclosed the claimed invention of '212 claim 1:

REDACTED

REDACTED

Mr. Valdes thus also admitted that all of the same elements of the '203 and '615 patent claims were present in *Emerald 1997*. The only additional limitation in these claims is the limitation of particular "categories" of network traffic (only ***one*** of which needs to be disclosed in order for a prior art reference to anticipate). But those limitations were inherently disclosed in *Emerald 1997* to one of ordinary skill in the art, or, at a minimum, would have been obvious in light of the express teaching in *Emerald 1997* to analyze those network traffic categories based upon the cited reference *Intrusive Activity 1991*.

While *Emerald 1997* was submitted to the Examiner during the prosecution of the '338, '212 and '615 patents, it was not considered during the '203 prosecution.[48] However, given the substantial overlap in text and figures between *Emerald 1997* and the patents' specification, as well as numerous admissions from SRI's inventors and expert, this reference so clearly impacts upon patentability that this fact should be considered virtually irrelevant.

1. Emerald 1997 describes all of the claimed inventions of the '212 patent

The overlap in figures and text between *Emerald 1997* and the patents' specification is striking, as shown in Exhibit W. Since '212 claim 1 is representative of many of the limitations present in the '203, '212 and '615 claims, a comparison of its limitations with the disclosure in *Emerald 1997* is instructive:[49]

---

[47] Valdes Tr. 466-67 [Ex. U]. *See also* admissions of SRI's expert Dr. Kesidis regarding *Emerald 1997* and the limitations of the hierarchical patent claims: Kesidis Tr. 670-72 (*Emerald 1997* discloses using network datagrams / IP packets for intrusion detection); 690-93 (*Emerald 1997* teaches deploying a plurality of monitors); 693-94 (*Emerald 1997* monitors generate reports of intrusions) [Ex. V].

[48] Kunin Decl. ¶¶ 17-19 [Ex. BB].

[49] The citations below are merely representative, and additional relevant quotes are

'212 Claim 1	**Disclosure in *Emerald 1997*** (emphasis added) **(*see also* Exhibit K)**
Method for monitoring an enterprise network, said method comprising the steps of:	EMERALD introduces a highly distributed, building-block approach to **network surveillance**, attack isolation, and **automated** response. *Emerald 1997* at 353. The typical target environment of the EMERALD project is a large **enterprise network** with thousands of users connected in a federation of independent administrative domains. *Id.* at 354.
deploying a plurality of network monitors in the enterprise network;	Service monitors are dynamically deployed within a domain… *Id.* at 355. All EMERALD monitors (service, domain, and enterprise) are implemented using the same monitor code base. *Id.* at 357. The basic analysis unit in this architecture is the EMERALD monitor, which incorporates both signature analysis and statistical profiling. *Id.* at 364.
detecting, by the network monitors, suspicious network activity	Multiple analysis engines implementing different analysis methods may be employed to **analyze a variety of event streams** that pertain to the same analysis target… The profiler and signature engines receive large volumes of event logs specific to the analysis target, and produce smaller volumes of **intrusion or suspicion reports** that are then fed to their associated resolver. *Id.* at 356.
based on analysis of network traffic data,	Underlying the deployment of an EMERALD monitor is the selection of a target-specific event stream. **The event stream may be derived from** a variety of sources including audit data, **network datagrams,** [50] SNMP **traffic,** application logs, and analysis results from other intrusion-detection instrumentation. … Event records are then forwarded to the monitor's analysis engine(s) for processing. *Id.* at 356. EMERALD also extends the statistical-profile model of NIDES, to analyze the operation of network services, network infrastructure, and activity reports from other EMERALD monitors. … the Network Security Monitor [7] seeks to analyze packet data rather than conventional audit trails… More recent work in UC Davis' GrIDS effort [24] employs activity graphs of network operations to search for traffic patterns that may indicate network-wide coordinated attacks. *Id.* at 364.
wherein at least one of the network monitors utilizes a statistical detection	EMERALD's profiler engine performs **statistical profile-based anomaly detection** given a generalized event stream of an analysis target (Section III-C). *Id.* at 356.

included in Exhibit K.

[50] As SRI's expert has admitted, a datagram is equivalent to a packet. Kesidis Tr. 670-72 [Ex. V].

'212 Claim 1	**Disclosure in *Emerald 1997*** (emphasis added) **(*see also* Exhibit K)**
method;	
generating, by the monitors, reports of said suspicious activity; and	EMERALD employs a building-block architectural strategy using independent distributed surveillance monitors that can **analyze and respond to malicious activity** on local targets, and can interoperate to form an analysis hierarchy. *Id.* at 355. The profiler and signature engines receive large volumes of event logs specific to the analysis target, and produce smaller volumes of **intrusion or suspicion reports** that are then fed to their associated resolver. *Id.* at 356.
automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	***Domain monitors* correlate intrusion reports disseminated by individual service monitors**, providing a domain-wide perspective of malicious activity (or patterns of activity). … **Enterprise-layer monitors correlate activity reports produced across the set of monitored domains**.... Through this **correlation and sharing of analysis results**, reports of problems found by one monitor may propagate to other monitors throughout the network. *Id.* at 356.

As detailed in the charts attached in Exhibit K, all of the dependent claim limitations for the '212 patent are also disclosed in *Emerald 1997*. Thus, the '212 patent is anticipated and therefore invalid.[51]

2. Emerald 1997 renders obvious and/or inherently anticipates all of the asserted claims of the '203 and '615 patents

According to both inventors, the only limitation in '203 claim 1 that is not disclosed verbatim in *Emerald 1997* are the claimed network traffic data categories.[52] These categories are, however, inherently disclosed. They are also an obvious addition.

Both inventors admitted that they were not the first to monitor ***many*** of the claimed categories of network traffic data (only ***one*** of which is needed for a prior art system to be an invalidating reference).[53] The inventors simply monitored the same types

[51] As shown in Ex. K, a similar analysis applies for '615 independent claims 34 and 44.

[52] Porras Tr. 434-39 [Ex. T]; Valdes Tr. 459-60 [Ex. U].

[53] Porras Tr. 289-95; 444-54 [Ex. T]; Valdes Tr. 283-87 [Ex. U]; *see also* Kesidis Tr.

of network traffic other computer systems and intrusion detection systems were already monitoring. The listed types of network traffic are the same as those that were already in use by network entities and other intrusion detection systems in the early 1990s.[54] Thus, these categories would have been inherent and/or obvious from the disclosure in *Emerald 1997* of the data sources for such categories – network datagrams and logs kept by network infrastructure.

a. Inherent anticipation (firewalls)

The doctrine of inherent anticipation applies when the evidence makes it clear that "the missing descriptive matter is necessarily present in the thing described in the reference, and it would be so recognized by persons of ordinary skill." *Continental Can Co.*, 948 F.2d at 1268. As explained previously, only one of the claimed network traffic data categories need be disclosed to anticipate the claims. Although *Emerald 1997* does not recite *ipsissimis verbis* the claimed network traffic data categories, several of these '203 and '615 claimed categories are necessarily present in the disclosure.

Two of the claimed "network traffic data categories" are "network connection requests" and "network connection denials." The patents' specification states that these categories involve monitoring (A) and (B):

> A. pass-through traffic (i.e., packets allowed into the internal network from external sources)

'338 col. 5:7-8 [Ex. A].

> B. discarded traffic (i.e., packets not allowed through the gateway because they violate filtering rules)

'338 col. 5:4-7 [Ex. A]. The specification discloses that such information can be gathered from the logs of network entities (also called network infrastructure)

383-84 [Ex. V].

such as routers, gateways, and firewalls:

> Event records can also be produced from other sources of network packet information such as report logs produced by network entities.

'338 col. 5:21-25 [Ex. A].

> Network entities include gateways, routers, firewalls…

'338 col. 3:43-44 [Ex. A].

Emerald 1997 makes the same disclosures as the patents. As shown previously, like the patents-in-suit, *Emerald 1997* disclosed that the EMERALD system monitored network traffic and network packets. Also like the patents-in-suit, *Emerald 1997* further disclosed that the EMERALD system monitored data from network infrastructure (network entities) such as gateways, routers, and firewalls:

> Service monitors are dynamically deployed within a domain to provide localized real-time analysis of **infrastructure** (e.g., routers or gateways) and services (privileged subsystems with network interfaces).

Emerald 1997 at 355 (emphasis added) [Ex. E].

> **network infrastructure** (e.g., routers, filters, DNS, **firewalls**)…

Id. at 354 (emphasis added) [Ex E]. The *Emerald 1997* paper also expressly disclosed collecting data for event records from activity logs, which to one of ordinary skill in the art would include firewall logs:[55]

> At the core of many signature-based expert systems exists an algorithm for accepting the input (in our case activity logs) and, based on a set of inference rules, directing the search for new information.

Id. at 355 [Ex. E]. Thus, *Emerald 1997* expressly taught analysis of data from network infrastructure such as a firewall, and the activity logs produced from a firewall.

Based upon these disclosures relating to firewalls and activity logs in *Emerald*

---

[54] Heberlein Decl. ¶¶ 53-58, 65-73 [Ex. Y].

[55] Avolio Decl. ¶¶ 42, 49-50, 53-54, 60, 67-71, 73 [Ex. X].

1997, one of ordinary skill in the art would have understood the monitoring of network connections to be necessarily present. A firewall is a security system that screens packet communications traveling across a particular network boundary that the firewall is set up to monitor.[56] Firewalls were common network components in 1997, and one of ordinary skill in the art would have been familiar with their configuration and operation.[57] As discussed in the Declaration of Frederick Avolio, firewalls in 1997 performed a set of common functions in monitoring and filtering packets, which would have been known to one of ordinary skill in the art at the time.[58]

When configuring a firewall, one ***must*** define what kinds of data pass through and what kinds of data are blocked – exactly the same data shown at (A) and (B) previously that the patent discloses for monitoring network connection requests and network connection denials.[59] Thus, a firewall must be configured to monitor: (1) network connection requests for packets that will be allowed to pass through the firewall ("pass-through traffic"); and (2) network connection denials of packets that violate the rules set up for entry ("discarded traffic"). In so doing, one necessarily monitors "network traffic data" corresponding to the "network connection requests and denials" categories listed in the '203 and '615 claims.

---

[56] *See* definition of "firewall" in *Computer Dictionary*, Microsoft Press 3rd ed. (1997) [Ex. LL].

[57] *See* Avolio Decl ¶ 42 [Ex. X].

[58] *See* Avolio Decl. ¶ 60 [Ex. X].

[59] "To set up your firewall, you must therefore define what kinds of data pass and what kinds are blocked. … *Default permit* With this strategy, you give the firewall the set of conditions that will result in data being blocked. Any host or protocol that is not covered by your policy will be passed by default. *Default deny* With this strategy, you describe the specific protocols that should be allowed to cross through the firewall, and the specific hosts that may pass data and be contacted. The rest are denied." S. Garfinkel and G. Spafford, PRACTICAL UNIX & INTERNET SECURITY at 638 [Ex. AA].

Firewalls in 1997 also routinely logged for review packets allowed in, and packets blocked or discarded.[60] Thus, the network packets for analyzing network connection requests and denials would have been present in a firewall's activity logs, which EMERALD used as a source of event data.[61] Thus, analysis of two of the "network connection requests/denials" embodiments disclosed by the patents naturally flow from the operation of the EMERALD system taught in *Emerald 1997*, and would have been recognized by one of ordinary skill at the time.[62]

An additional claimed category of "network traffic data" is "network packet data volume."[63] A standard firewall in 1997 monitored the amount of packet data sent over each connection.[64] Because it was standard practice for firewalls to monitor and log the

---

[60] *See* D. B. Chapman and E. Zwicky, BUILDING INTERNET FIREWALLS, at 179-80: "Make sure the packet filtering router gives you the option of logging all of the packets it drops. ...You'd also like to be able to log selected packets that were accepted. For example, you might want to log the start of each TCP connection." *See also id.* at 400: "In particular, you want to log the following cases:

All dropped packets, denied connections, and rejected attempts

At least the time, protocol, and user name for every successful connection to or through your bastion host

All error messages from your routers, your bastion host, and any proxying programs." [Ex. DD].

[61] Kesidis Tr. 688-89 (admitting firewalls logged blocked packets, which could indicate a connection attempt) [Ex. V].

[62] *See* Avolio Decl. ¶¶ 61-71 [Ex. X].

[63] In construing these terms, one looks first to the words of the claim terms themselves, which are "generally given their ordinary and customary meaning." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). The plain meaning of "network packet data volume" is any information illustrating the size of a particular set of network traffic. The patent specification explicitly states that the number of packets and the number of bytes constitute "event records" for the analysis engines. *See* '338 col. 5:30-35, 6:1-5 [Ex. A]. *See also* Kesidis Tr. 564-65 [Ex. V]; Valdes Tr. 179-80 [Ex. U].

[64] "A firewall can be used to monitor communications between your internal network and an external network. For example, you could use the firewall to log the endpoints and **amount of data** sent over every TCP/IP connection between your organization and the outside world." S. Garfinkel and G. Spafford, PRACTICAL UNIX & INTERNET SECURITY at

number of packets and kilobytes of data transferred over each particular connection, one of ordinary skill in the art would have recognized such monitoring as an inherent feature of setting up an EMERALD-type system.[65]

As detailed in the charts attached in Exhibit K, all of the dependent claim limitations for the '203 and '615 patents are also disclosed in *Emerald 1997*. Thus, the '203 and '615 patents are anticipated and therefore invalid.[66]

b. Obvious to combine Emerald 1997 with an internally cited reference

Emerald 1997 explicitly states that the EMERALD system monitors "network datagrams" (known at the time to be network packets).[67] *Emerald 1997* goes on to explain that another intrusion detection system, the Network Security Monitor ("NSM"), also analyzed packet data, and directs the reader to a paper on NSM, cited reference [7]. *See Emerald 1997* at 364 [Ex. E], citing to L.T. Heberlein et al., *A Method to Detect Intrusive Activity in a Networked Environment*, 14th National Computer Security Conference, Oct. 1-4, 1991 ("*Intrusive Activity 1991*") [Ex. F]. SRI's expert Dr. Kesidis conceded that *Emerald 1997* directed one of skill in the art to look to the *Intrusive Activity 1991* reference to find out more about analyzing packet data.[68] Thus, *Emerald 1997* expressly provided the motivation to combine the two references. *See In re Saunders*, 444 F.2d 599, 603 (C.C.P.A. 1971) (sustaining an obviousness rejection involving the combination of an internally-cited reference, and noting "it would not have been necessary for one skilled in the art to have gone any further than another part of [the

---

639 (emphasis added) [Ex. AA].

[65] *See* Avolio Decl. ¶¶ 72-78 [Ex. X].

[66] As shown in Exhibit K, a similar analysis applies for '615 independent claims 34 and 44.

[67] *Emerald 1997* at 356 [Ex. E]; Kesidis Tr. 670-72 [Ex. V].

[68] Kesidis Tr. 673-76 [Ex. V]; *see also* Porras Tr. 424-25 [Ex. T].

cited reference] to find the specified proportions of the appealed claims.").[69]

Like the patent specification's disclosure on abstracting raw network packet data into "events," *Intrusive Activity 1991* describes a method for analyzing network activity by developing representative "objects" from information in network packets. *See Intrusive Activity 1991* at 364 [Ex. F]. In particular, *Intrusive Activity 1991* defines parameters to monitor in a stream, or individual connection, composed of packets. *Id.* at 368 [Ex. F]. Two parameters explicitly called out are "the number of packets" and the "number of bytes" – both of which constitute a measure of "network packet data volume." *Id.* at 368-69 [Ex. F].[70] This is one of the network traffic categories listed in the '203 and '615 patent claims.

In addition, *Intrusive Activity 1991* discloses other measures listed in the claimed categories such as network connection requests and denials. For example, it explains that "network connections are ***created*** and ***destroyed*** continuously," *id.* at 365 (emphasis added) [Ex. F], and notes that:

> We have concentrated our analysis efforts on **isolated behavior-detection functions for connections.** ... The higher the suspicious value is, the more likely our monitor believes the connection is associated with intrusive activity. We monitored the Electrical Engineering and Computer Science LAN at UCD for a period of approximately three months. **During this time over 400,000 connections were detected and analyzed**, and among these connections, over 400 were identified as being associated with intrusive behavior.

---

[69] Some courts have held that internally-cited references satisfy anticipation as well, *see, e.g., Rheox, Inc. v. United Catalysts, Inc.*, 1995 U.S. Dist. LEXIS 13054 (D. N.J. 1995) (unpublished) (stating "consideration of a reference within a reference is consistent with the established standards for determining anticipation.") [Ex. PP].

[70] *See supra* note 63.

Id. at 370 (emphasis added) [Ex. F]. One of ordinary skill would have understood this disclosure of analyzing the creation and destruction of network connections to disclose monitoring "network connection requests" and "network connection denials."

Thus, *Emerald 1997* in combination *with Intrusive Activity 1991* renders obvious the claims of the '203 and '615 patents which require monitoring one or more particular categories of network traffic. As shown in Exhibit K, the rest of the dependent claim limitations for these patents are also disclosed in *Emerald 1997*.

3. Emerald 1997 is enabled

SRI suggests that *Emerald 1997* was merely a vague proposal that did not enable any of the claimed inventions.[71] But *Emerald 1997* is not a mere proposal – it is a detailed, peer-reviewed article published and presented at a conference proceeding. Given the striking similarities in detail between the patent specification and *Emerald 1997*,[72] SRI cannot simultaneously claim that the text in *Emerald 1997* is not enabling, while contending that the same text is enabling in the patent specification. If the patents-in-suit are enabled, so too is *Emerald 1997*.[73]

SRI has argued that *Emerald 1997* does not provide an "enabling disclosure of a statistical detection method."[74] To the extent any information about statistical detection methods is believed to be missing from *Emerald 1997*, it would have been obvious to combine *Emerald 1997* with its internally cited reference [9] for the same reasons discussed above regarding *Intrusive Activity 1991*. *See* H.S. Javitz and A. Valdes, *The*

---

[71] Porras Tr. 433 (referring to *Emerald 1997* as an "early conceptual design") [Ex. T]; Kesidis Tr. 696 (describing *Emerald 1997* as a "research proposal") [Ex. V].

[72] *See* Ex. W.

[73] *See* Heberlein Decl. ¶¶ 89-93 [Ex. Y].

[74] *See* SRI's Amended Response to Symantec's Invalidity and Inequitable Conduct Contentions [Ex. MM].

NIDES statistical component description and justification, Technical report, Computer Science Laboratory, SRI International, Menlo Park, CA, March 1994 ("*NIDES 1994*") [Ex. G]. *Emerald 1997* states that *NIDES 1994* describes "the NIDES statistical profile-based anomaly-detection subsystem (NIDES/Stats), which employed a wide range of multivariate statistical measures to profile the behavior of individual users." *Emerald 1997* at 359 [Ex. E]. *Emerald 1997* also explains that the NIDES mechanisms "are well suited to the problem of network anomaly detection, with some adaptation." *Emerald 1997* at 359 [Ex. E]. Thus, if one of ordinary skill in the art needed further details in order to practice EMERALD's statistical detection methods, *Emerald 1997* explicitly directed one of ordinary skill to NIDES statistical profiling papers, such as *NIDES 1994* or *Statistical Methods*, just like the patent specification, which also directed one skilled in the art to *Statistical Methods*. '338 col. 5:42-48 [Ex. A].

C. The Live Traffic Publications Anticipate or Render Obvious the Asserted Claims

Defendants rely on two different versions of the same *Live Traffic* paper: an HTML version published on-line more than one year prior to the filing date,[75] (*see* Ex. I) and a Symposium version published prior to the filing date (*see* Ex. H),[76] as invalidating prior art. *Live Traffic* was submitted to the US PTO during the '212 and '615 prosecutions, but it was not considered by the US PTO during the prosecution of the '338 and '203 patents.[77]

---

[75] The HTML version is the version that comes up when one clicks on the relevant link on the SRI webpage. Porras 30(b)(6) Tr. 120-21 [Ex. T].

[76] The actual text of *Live Traffic* is the same between the HTML and Symposium proceeding formats.

[77] Kunin Decl. ¶¶ 15-16 [Ex. BB].

1. Live Traffic (HTML version) was publicly available prior to November 9, 1997

Prior to the November 9, 1997 102 (b) date, SRI published *Live Traffic* on the Internet in two places – an ftp site and on the SRI website.[78] When Mr. Porras submitted this paper for consideration to the Internet Society Symposium's committee on August 1, 1997, he also

REDACTED

This ftp site was a publicly-available website that Mr. Porras advertised to researchers in the intrusion detection field as a place where they could find information on EMERALD.[80] For example, in a presentation dated February 5, 1997, Mr. Porras pointed to documents that could be found at the ftp site:[81]

REDACTED

On August 1, 1997, the same day Mr. Porras submitted *Live Traffic* for consideration by the Symposium, he also published an HTML version of the paper on SRI's worldwide website.[83] Mr. Porras testified that he remembered loading the HTML version of the *Live Traffic* paper on the website and that he believed it would have the

---

[78] An "ftp" site is a network location from which files can be downloaded using a "file transfer protocol."

[79] Porras 30(b)(6) Tr. 110-12 and Porras Exhibit SRI-26 (SRIE 0460761) [Ex. T].

[80] Porras 30(b)(6) Tr. 16-17, 47-50, 57-61[Ex. T].

[81] Porras 30(b)(6) Tr. 44-48 and Porras Exhibit SRI-3 (SRI 105589-609 at SRI 105590) [Ex. T].

[82] Porras 30(b)(6) Tr. 48 [Ex. T].

[83] Porras 30(b)(6) Tr. 110-22 and Porras Exhibit SRI-27 (SRI 094295) (SRI document showing current website downloads of the EMERALD project in August 1997, which lists *Live Traffic* (HTML version) as being available for download on August 1, 1997) [Ex. T].

same content as the version that was published in the Symposium.[84]

These public postings of *Live Traffic* make it a "printed publication" under 35 U.S.C. § 102 (b). The key inquiry as to whether something is a printed publication is whether the reference is publicly accessible to the public interested in the art. *See In re Klopfenstein*, 380 F.3d 1345, 1348 (Fed. Cir. 2004). Here, *Live Traffic* was available on SRI's publicly accessible website. In addition, SRI had informed the relevant public, researchers in the intrusion detection field, that EMERALD information was posted on both the ftp site and the SRI worldwide website. "If accessibility is proved, there is no requirement to show that particular members of the public actually received the information." *Constant* v. *Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1568 (Fed. Cir. 1988).

2. Live Traffic (HTML version) anticipates or renders obvious the asserted claims under 35 U.S.C. 102 (b)

Live Traffic provides additional details and examples of network traffic monitoring and the statistical algorithms used in EMERALD. *See, e.g., Live Traffic* at 5-7 [Ex. I]. Like *Emerald 1997*, there is substantial overlap in the figures and text between *Live Traffic* and the patents' specification.[85] As shown in Exhibit L, *Live Traffic* anticipates all of the asserted claims of the patents-in-suit. Indeed, SRI has not even contested the anticipation of any of the independent claims by *Live Traffic*.[86]

To the extent any of the dependent claims are not anticipated by *Live Traffic*, it would have been obvious to combine *Live Traffic* with *Emerald 1997*. *Live Traffic*

---

[84] Porras 30(b)(6) Tr. 120-21 [Ex. T].

[85] Compare *Live Traffic* figure p. 14 with '338 Fig. 1; *see also Live Traffic* p. 10 and '338 col. 6:59-7:3.

[86] *See* SRI's Amended Response to Symantec's Invalidity and Inequitable Conduct Contentions [Ex. MM]; *see also* Kesidis Tr. 147 (admitting *Live Traffic* teaches some of

specifically cites to *Emerald 1997* at reference [20], *Live Traffic* at 22 [Ex. I], and explicitly points the reader to *Emerald 1997* for further information:

> This paper takes a pragmatic look at the issue of packet and/or datagram analysis based on statistical anomaly detection and signature-analysis techniques. This work is being performed in the context of SRI's latest intrusion-detection effort, EMERALD, a distributed scalable tool suite for tracking malicious activity through and across large networks [20].

Live Traffic at 3 [Ex. I]. Thus, for the reasons discussed above with regard to *Intrusive Activity 1991*, it would have been obvious to combine *Live Traffic* and *Emerald 1997*. The chart in Exhibit L includes citations to *Emerald 1997* indicating claims that in the alternative are rendered obvious by this combination.

3. Live Traffic (Symposium version) also anticipates or renders obvious the asserted claims under 35 U.S.C. 102 (a)

SRI also published *Live Traffic* in the March 1998 Internet Society's Networks and Distributed Systems Security Symposium proceedings.[87] This March 1998 version of *Live Traffic* contains identical text to the HTML version of *Live Traffic*. Thus, for the reasons noted above, *Live Traffic* also invalidates the asserted claims under 35 U.S.C. § 102 (a).

D. THE JINAO REPORT ANTICIPATES THE ASSERTED CLAIMS

The *JiNao Report* was publicly available more than one year before the filing date of the patents-in-suit.[88] The *JiNao Report* described the architecture of an intrusion detection system designed for protecting against intrusions into network infrastructure such as routers. *See JiNao Report* at 1 [Ex. J]. The JiNao system performs both statistical and signature analysis of network routing and management protocol traffic.

---

the claims) [Ex. V].

[87] *See* Ex. H.

[88] *See supra* note 30.

See JiNao Report at 1 [Ex. J].[89] The JiNao system's "dual analysis engine" monitor is quite similar to the dual analysis engine monitor shown in Fig. 2 of the patent specification.[90] Both monitors read in network traffic and perform statistical analysis upon that traffic looking for intrusions. In addition, both monitors use the same NIDES statistical profiling algorithms adapted for network traffic.[91]

The *JiNao Report* was not submitted to the US PTO or considered by the Examiner for any of the patents-in-suit.

1. The JiNao Report anticipates the asserted '338 claims

As shown in Exhibit M, the *JiNao Report* anticipates all of the asserted claims of the '338 patent. SRI's expert Dr. Kesidis conceded that the system described in the *JiNao Report* satisfies all of the elements of '338 claim 1:

- JiNao received network packets handled by a network entity,[92]
- JiNao built long-term statistical profiles,[93]
- JiNao built short-term statistical profiles,[94]
- JiNao used measures of network packets[95] monitoring network connections,[96]
- JiNao compared a long-term and a short-term statistical profile,[97]
- JiNao determined whether there is a significant difference between the

---

[89] Jou Tr. 24-25 [Ex. R].

[90] Compare *JiNao Report* Figure 1 at 4 with '338 Fig. 2. and '338 col. 4:48-60.

[91] *See JiNao Report* at 18 [Ex. J] and '338 col. 5:43-52 [Ex. A].

[92] Kesidis Tr. 50-51, 55-58 [Ex. V].

[93] Kesidis Tr. 52-53, 58 [Ex. V].

[94] Kesidis Tr. 53, 58 [Ex. V].

[95] Kesidis Tr. 210-212 [Ex. V].

[96] Kesidis Tr. 51, 58-59 [Ex. V]. Specifically, Dr. Kesidis conceded that the Hello packets which JiNao monitored indicate a network connection. The *JiNao Report* at 19 discloses that JiNao monitored Hello packets.

[97] Kesidis Tr. 53, 59 [Ex. V].

profiles.[98] A significant statistical deviation indicates an alert.[99]

SRI appears to be attempting to distinguish the *JiNao Report* as not satisfying the claim preamble requiring a "method of network surveillance."[100] However, a claim preamble is not a limitation of the claim if it merely recites a statement of purpose. *See Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F. 3d 1298, 1305 (Fed. Cir. 1999). Furthermore, SRI's expert conceded the actual claimed method was laid out in the method steps, not the preamble.[101] SRI never previously claimed this preamble constituted a claim limitation, and never requested construction of any of the terms in the preamble.[102]

However, even assuming the preamble constitutes a claim limitation, the disclosed JiNao system satisfies it. As SRI's expert admitted, the JiNao monitor receives packets from the network.[103] Furthermore, the *JiNao Report* itself makes it clear the system is designed for performing network surveillance:

> In particular, we will conduct logical and statistical **analysis of network routing and management protocols** to construct a scalable distributed intrusion detection system for the emerging internetwork environment.

JiNao Report at 1 (emphasis added) [Ex. J].

> Most of the current **network intrusion detection efforts** have taken one of the two following approaches. One approach is to collect data from separate hosts on a network for processing by a centralized intrusion

---

[98] Kesidis Tr. 54 [Ex. V].

[99] Kesidis Tr. 74 [Ex. V].

[100] Kesidis Tr. 47-50 [Ex. V].

[101] *See* Kesidis Tr. 396 [Ex. V].

[102] *See* D.I. 265 (SRI's Opening Claim Construction Brief).

[103] Kesidis Tr. 210-11 [Ex. V]; *see also JiNao Report* at 4 (Fig. 1) (showing the statistical analysis portion of the local detection module receives data from the network, and at 18, stating "[a]fter the incoming packet passes through the rule-based checking, it will be forwarded in parallel both to the protocol engine for execution and to the detection module for further analysis."). [Ex. J].

> detection system [2][3]. The other approach is **to target network traffic at the service and protocol levels** [6][7]. **Our effort is close to the second approach** with a few exceptions.

JiNao Report at 2 (emphasis added) [Ex. J].

In addition to disclosing using measures monitoring "network connections" for statistical profiling, the *JiNao Report* further disclosed using measures satisfying '338 claims 2, 4 and 5. The *JiNao Report* disclosed the monitoring of different types of OSPF packets, several of which correspond to the claimed measure categories. *See JiNao Report* at 19 [Ex. J]. For example, the monitored "Link State Request" packets are used to request up-to-date pieces of a neighbor's database, and thus constitute a "network packet data transfer command" as required by '338 claim 2.[104] The monitored "Hello" packets are sent periodically to establish and maintain neighbor relationships, or connections, and thus constitute both a measure of "network connections" and also a "network connection request" as required by '338 claim 5.[105]

In addition, the *JiNao Report* also directs the reader to monitor "network packet data transfer volume" as required by '338 claim 4. For example, the *JiNao Report* states:

> The activity intensity measures determine whether the **volume of general activity** generated in the recent past (depending on the half-life of the measure, here "recent past" corresponds to the time span of last several half-lifes) is normal.

JiNao Report at 19 (emphasis added) [Ex. J]. One of the authors of the *JiNao Report*, Mr. Jou, agreed that this text disclosed using data volume as a measure.[106] Thus, as shown in Exhibit M, all of the asserted '338 claims are invalided by the *JiNao Report*.

---

[104] *See* RFC 2328 <http://www.ietf.org/rfc/rfc2328.txt?number=2328> at SYM_P_0604975 (describing Link State Request packet) and at SYM_P_0604583-604 (describing OSPF packets generally) [Ex. OO].

[105] *Id.* at SYM_P_0604967 (describing OSPF Hello packets) [Ex. OO].

[106] Jou Tr. 164-65 [Ex. R].

2. The JiNao Report anticipates the asserted hierarchical claims

The *JiNao Report* also anticipates the asserted hierarchical claims of the '203, '615 and '212 patents. It disclosed a modular architecture using the same two types of analysis engines as disclosed in the SRI patents – a NIDES-like statistical detection engine and a signature-based analysis engine. *See JiNao Report* Fig. 1 at 4 [Ex. J]. As shown in Fig. 1, the lowest-level JiNao monitors (described as a "Local JiNao") analyze packets, while the higher-level monitors (described as "Remote Management Applications") analyze the results of Local JiNao monitors. *Id.* The hierarchical monitors are shown as including the same generic analysis engines – a statistical detection engine and a signature-based analysis engine – as the lower-level monitors. *Id.*

The *JiNao Report* also disclosed that the information from lower-level monitors could be integrated and correlated at a higher-level monitor for intrusion detection:

> [A] higher-level decision module, i.e. one that has access to observations on a larger topological region, can correlate multiple detections from low-levels according to their respective scope of impact, and to reach a more accurate detection decision.

Id. at 32. In addition, the *JiNao Report* also explained that the JiNao modules' architecture allowed the system to scale to a regional or global hierarchy. *Id.* at 13. As shown in the chart attached at Exhibit M, all of the limitations of all of the asserted claims are disclosed by the *JiNao Report*, and thus the asserted claims are anticipated.

V. CONCLUSION

Since the systems and methods claimed in the asserted claims of the '338, '203, '212, and '615 patents were described in printed publications more than one year before their date of application for patent, Defendants are entitled to summary judgment pursuant to 35 U.S.C. § 102 and 103 that the claims are invalid as a matter of law.

Dated: June 23, 2006

POTTER ANDERSON & CORROON LLP

/s/ Richard L. Horwitz
Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600
Fax: (404) 572-5134

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC.,
a Delaware Corporation and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia Corporation

MORRIS, JAMES, HITCHENS & WILLIAMS, LLP

/s/ Mary B. Matterer
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800

OF COUNSEL:

Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Blvd.,
Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

CERTIFICATE OF SERVICE

I hereby certify that on the 23rd day of June, 2006, I electronically filed the foregoing document, **REDACTED VERSION OF OPENING BRIEF IN SUPPORT OF JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103 OF DEFENDANTS ISS AND SYMANTEC,** with the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 23rd day of June, 2006, the foregoing document was served via email on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
1180 Peachtree Street
Atlanta, GA 30309-3521
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/ Mary B. Matter
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com
Counsel for Symantec Corporation